(12) UK Patent Application (19) GB (11) 2 408 129 (13) A

(43) Date of A Publication 18.05.2005

(21) Application No: 0326594.9

(22) Date of Filing: 14.11.2003

(71) Applicant(s):
iSolve Limited
(Incorporated in the United Kingdom)
78A King Street, KNUTSFORD, Cheshire,
WA16 6ED, United Kingdom

(72) Inventor(s):
Marc Poulaud
Nigel Elson

(74) Agent and/or Address for Service:
Lloyd Wise, McNeight & Lawrence
Highbank House, Exchange Street,
STOCKPORT, Cheshire, SK3 0ET,
United Kingdom

(51) INT CL[7]:
G06F 1/00

(52) UK CL (Edition X):
G4H HJ H2B

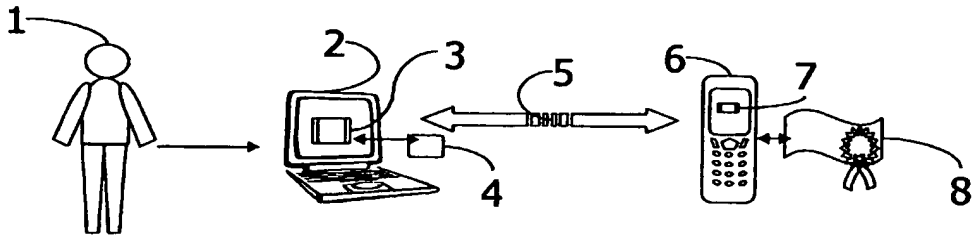
(56) Documents Cited:
WO 2002/095689 A1
WO 2000/031608 A2
US 20020078362 A1
WO 2002/032151 A2
JP 100228327 A

(58) Field of Search:
UK CL (Edition X) G4H
INT CL[7] G06F
Other:

(54) Abstract Title: **User authentication via short range communication from a portable device (eg a mobile phone)**

(57) A user is authenticated to a computing device (PC) 2 by the transmission of 'credentials' 8 (user ID biometric etc') from a mobilephone 6 (or the like) device via a short range communication link 5 such as 'Bluetooth,' IrDa or WiFI. The user may have to input information for authentication at the mobilephone, for example the mobile phone may include a fingerprint scanner to scan the user's finger. The phone may be used to form a virtual private network.

Figure 1



GB 2 408 129 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

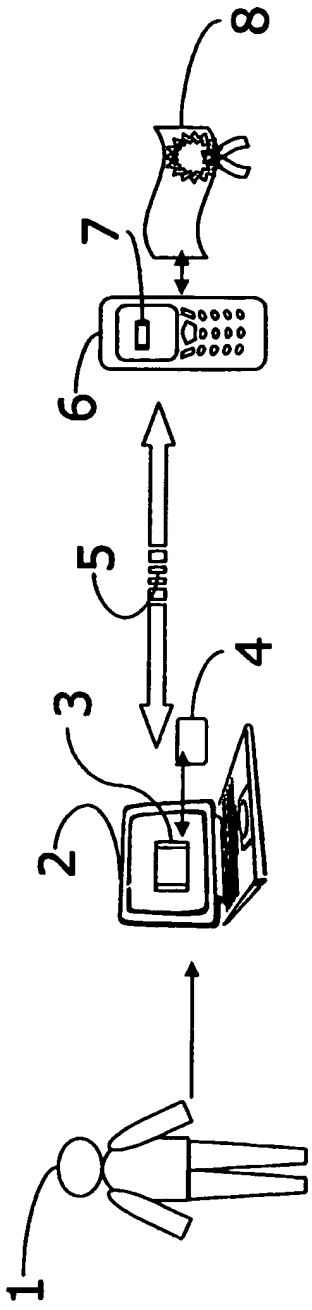


Figure 1

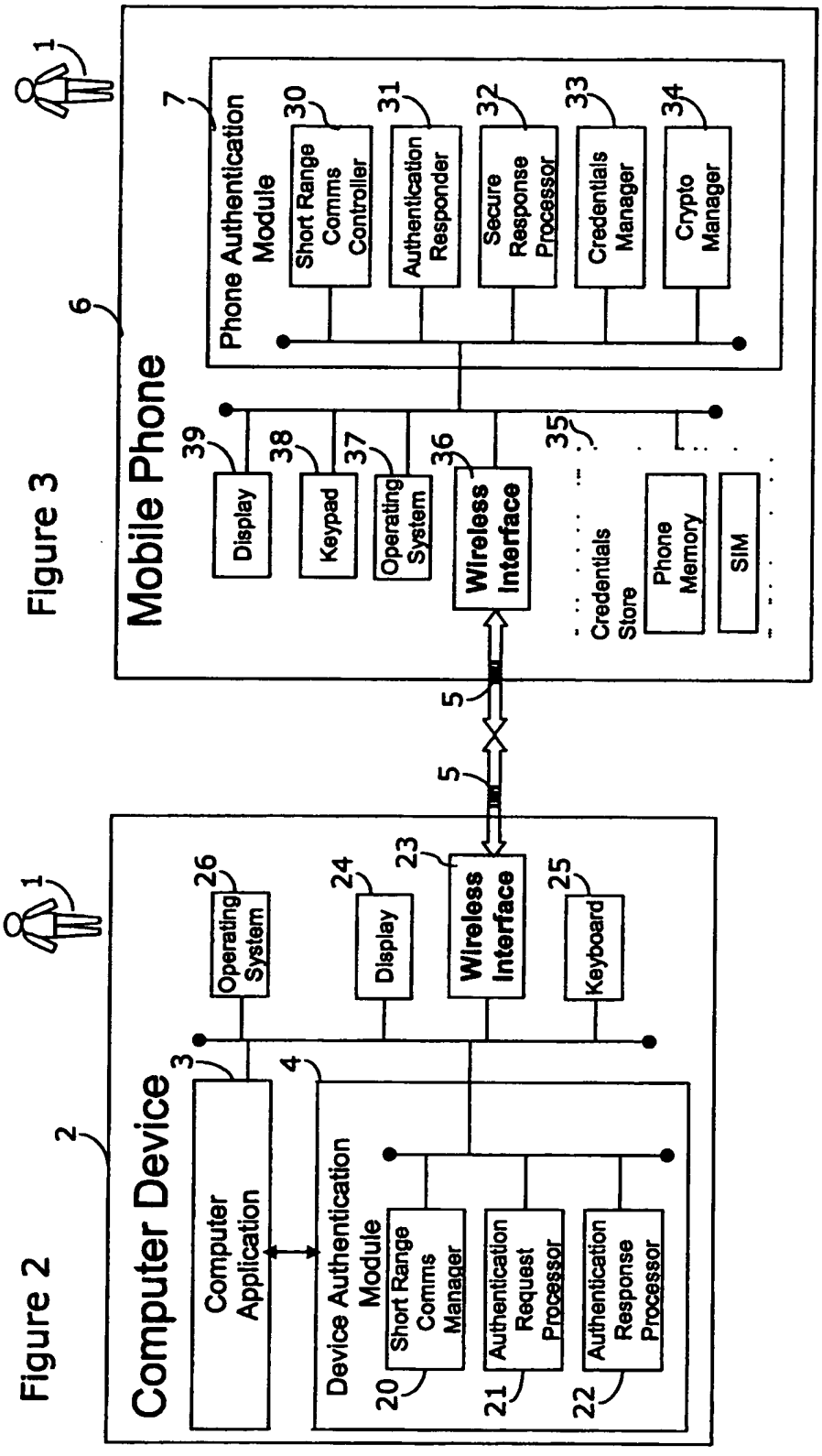


Figure 2
Computer Device
2
1
Computer Application
3
Operating System
26
Device Authentication Module
4
Short Range Comms Manager
20
Authentication Request Processor
21
Authentication Response Processor
22
Display
24
Wireless Interface
23
Keyboard
25
5
5
Figure 3
Mobile Phone
6
1
Phone Authentication Module
7
Short Range Comms Controller
30
Authentication Responder
31
Secure Response Processor
32
Credentials Manager
33
Crypto Manager
34
Display
39
Keypad
38
Operating System
37
Wireless Interface
36
Credentials Store
35
Phone Memory
SIM

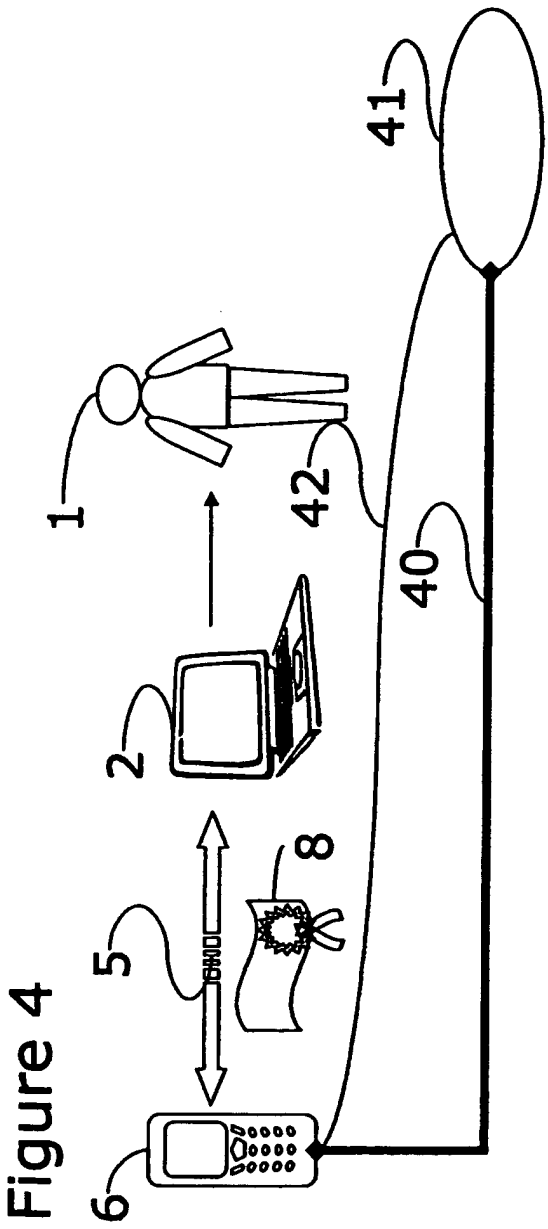


Figure 4

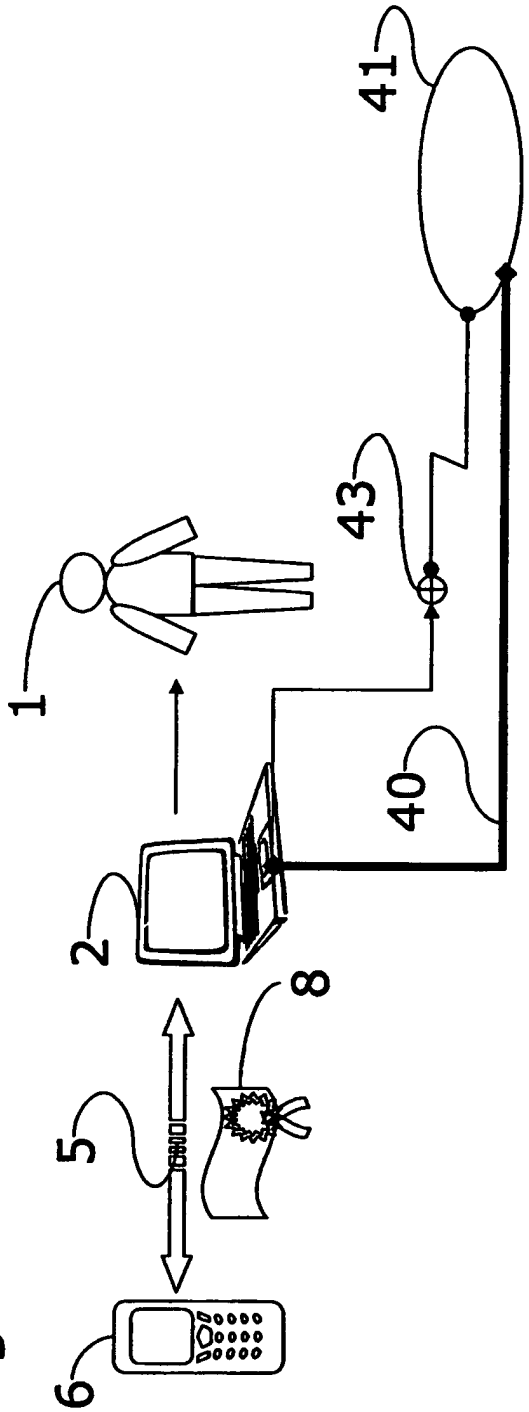


Figure 5

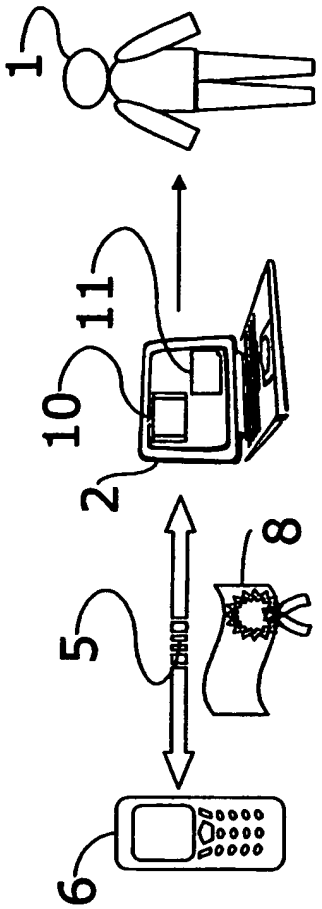


Figure 6

User Authentication Device

The present invention is concerned with improved apparatus, systems and methods for effecting authentication to a computer application, particularly by means of a short-range wireless connection. In particular, the identity of a user can be authenticated to a computer application.

In order to effect "strong authentication" of a user to a computer application, the user is required to be in possession of a number of identification factors. The more factors that are required, and particularly the greater the number of different types of authentication factors required, the greater the level of authentication which can be attributed to the user. Examples of such "factors" are knowledge of at least one secret, possession of a hard token, and biometric information. Examples of secrets are a user name and password, and digital certificates and asymmetric cryptographic keys, and symmetric cryptographic keys. Hard tokens are physical media for storing electronic credentials and include smart card devices, USB tokens and one-time password devices. Biometrics include fingerprint scans, retina scans, hand scans, signature scans, voice scans, iris scans, facial scans and keystroke scans.

Each of the individual identification factors has its own strengths and weaknesses. For example, one-time password devices provide a time-limited authentication to a computer, meaning that a third party who copies the password and subsequently uses it outside of the time-limited period (typically no more than a minute or two in duration) will find it to be invalid. However, it is possible for such devices to be stolen and used by unauthorised parties. Therefore some aspects of the device make it highly secure, other aspects mean that it is best combined with another identification factor in order to enhance the level of

authentication it provides. Thus for example it might be combined with possession of a use name and/or password, or with biometric data such as an iris scan.

However, one disadvantage of such devices, and particularly two-factor devices, is that they require some form of physical reader to be attached to the computer on which the authenticating application is running. Thus for example a smart-card reader or a biometric device may be attached to the computer.

Thus in the case of a portable computer device a user may have to carry with them not only the computer device itself (e.g. a laptop computer), but also the appropriate reader. In the case of USB type tokens, although they can be plugged directly into a computer's USB socket, they are still a cause of inconvenience since they must be physically connected to the computer and are an additional item which must be carried by the user and which is relatively easy to forget or lose.

In the case of one-time password devices, although they are smaller than reader devices such as biometric readers, they have the substantial disadvantage of requiring a network connection in order to communicate with a remote authentication server to determine whether the information supplied is valid. The use of such systems is also relatively complex and expensive, requiring additional systems hardware and expenditure of resources on configuration and maintenance.

It is known in the prior art to use mobile phone devices as part of an authentication system. For example, US 2001/0031637 discloses the use of a mobile phone device to authenticate itself to a remote information processing apparatus (e.g. a remote network). WO 02/095689 discloses an access control system which uses a mobile phone device to authenticate a user to an access control device which then provides access for a user's computer to a protected function. WO 01/99369 discloses the authentication of electronic

devices to one another over a short-range wireless link when a user enters authentication information into each device. The devices can then authenticate one another over an alternative communication link (e.g. a long-range network connection). GB 2369205 discloses a personal data device (e.g. mobile phone) and protection system with deletion of contents, the device securely storing data for a user and deleting it upon any failure of authentication. The securely stored data can also be stored remotely (e.g. on a networked database server) in order that deleted data can be recovered. US 2001/0052075 concerns methods and systems for connecting devices to one another using authentication codes which ensures that when connected, the devices only communicate with one another. EP 1168870 concerns an improved method for authentication of a user subscription identity module of a mobile phone over a mobile phone network. WO 02/03177 is concerned with verifying the identity of a person seeking access to a computer on a network by using the person's mobile phone and its unique identification characteristics - its phone number (provided by e.g. a SIM card) and identifiable by the party receiving a call, and its unique identification (UID) number for which the mobile phone can be interrogated across the mobile phone network to which it is connected.

However, none of the prior art authentication devices or systems meet all of the following requirements:

i) no need for a user to carry additional hardware;

ii) provision of authentication where there is no mobile phone network coverage;

iii) low cost of acquisition;

iv) easy and inexpensive integration with existing security systems;

v) wireless provision of authentication data from a hard token to an authenticating computer device; and

vi) storage on a single authentication device of multiple sets of authentication data.

The present invention seeks to overcome the abovementioned prior art disadvantages. According to the present invention there is provided apparatus for effecting authentication to a computer device, comprising:

(a) a computer device comprising:

(i) short-range wireless communication means; and

(ii) program means comprising a computer device authentication module for communicating with a remote device using said short-range wireless communication means and authenticating said remote device;

(b) a portable communication device comprising:

(i) mobile phone network communication means;

(ii) short-range wireless communication means;

(iii) program means comprising a portable communication device authentication module for communicating with said computer device using said short-range wireless communication means; and

(iv) data storage means providing a credentials store for storing authentication data.

The present invention makes use of portable communication devices which, in their simplest form, can consist just of a telephone device. However, other devices can be used which incorporate mobile phone technology to allow them to communicate *via* a mobile phone (cell phone) network, but which provide additional functionality. Thus for example the portable communication device may be a PDA device having mobile phone functionality, or a Nextel Blackberry (RTM) device incorporating short-range wireless communication means, or a portable communication device provided with an operating system such as the Symbian (RTM) OS or the Microsoft WindowsCE (RTM) OS.

The mobile phone network communication means may be any means which can effect communication with a mobile phone (or cell phone) network. For example, communication may be effected using equipment and protocols so as to effect communication with a 2G or 3G mobile phone network, for example using CDMA and WCDMA protocols etc. as appropriate. The portable communication device may therefore additionally comprise a SIM card.

The present invention provides for a wide range of applications using the authentication data. For example, not only may a user be authenticated to the computer device, but the portable communication device with its authentication data may also be used to digitally sign data. Thus for example a user may input data into the computer device, which can then transmit it to the portable communication device using the short-range wireless communication means, and the portable communication device can digitally sign the data using the authentication data, and the signed data can then be returned to the computer device and the data used as appropriate. Thus the portable communication device can be used not only to authenticate a user to the computer device, but also to digitally sign data for the purposes of data origin authentication.

In its various embodiments, the present invention particularly relates to the authentication of a user to a computer device.

Also provided according to the present invention is a method for effecting authentication to a computer device using a portable communication device, said computer device comprising:

(i) short-range wireless communication means;

(ii) program means comprising a computer device authentication module for communicating with a remote device using said short-range

wireless communication means and authenticating said remote device; and

(iii) data storage means for storing reference data against which authentication is to be effected;

and said portable communication device comprising:

(i) mobile phone network communication means;

(ii) short-range wireless communication means;

(iii) program means comprising a portable communication device authentication module for communicating with said computer device using said short-range wireless communication means; and

(iv) data storage means providing a credentials store for storing authentication data;

said method comprising the steps of:

(a) transmitting a request for electronic credentials *via* said short-range communication means from said computer device to said portable communication device;

(b) with said portable communication device authentication module, processing said request for electronic credentials, determining a response to said request for electronic credentials based upon said authentication data, and executing said response; and

(c) with said computer device, processing said response to said request for electronic credentials to determine an authentication state.

Thus identification data is stored on the portable communication device and reference data is stored on the computer device. Authentication of the portable communication device to the computer device is effected using the short-range wireless communication means and does not require any kind of additional network connection to be effected. Thus a fundamental problem encountered with authentication systems which use remote

authentication servers is bypassed - the present invention does not require a network connection e.g. over a mobile phone network in order for authentication to be effected. This is particularly useful when a user is outside of their mobile phone service provider's area of network coverage. The cost and inconvenience of running remote authentication servers across a network is also avoided. Furthermore, authentication is effected via standard wireless communication means shared by the computer device and portable communication device, and requires a user to only have the computer device and a portable communication device, the portable communication device (such as a mobile phone) being a standard piece of equipment carried by an increasingly large proportion of the population. This bypasses the need to carry cumbersome, inconvenient, expensive and easily forgettable tokens and authentication equipment such as USB tokens, smart cards and smart card readers etc.

The computer device can be any desired computer device such as a laptop or hand held PC which may e.g. run a range of applications or not be restricted to running specific applications. Thus for example the computer device may run a standard operating system such as Windows (RTM), Linux (RTM), PalmOS (RTM) etc. Alternatively, it may be a computer device which is configured to run only specific programs and perform only specific tasks. For example, the computer device may be a building access control device running a proprietary operating system.

The short-range wireless communication means may use any desired short-range wireless communications system. Standard systems include Bluetooth (RTM), IrDA and WiFi. Thus short-range electromagnetic systems may use Infra Red signals (IrDA) or signals in other parts of the electromagnetic spectrum as appropriate.

The computer device authentication module is configured to communicate *via* the short-range wireless communication means with the portable communication device

authentication module. The communication between the computer device and the portable communication device is to effect the exchange of data in order to validate the identity of the portable communication device (e.g. a mobile phone) to the computer device. For example, data can be exchanged between them in an unencrypted format. Alternatively, the computer device and portable communication device can effect a key exchange of the public parts of public-private key pairs, and can then encrypt data for one-another using the other device's public key. A wide range of systems, conventions and protocols are well known in which the secure exchange of data can be effected between devices using asymmetric cryptographic algorithms.

Alternatively, the devices can be pre-registered with one another (for example a key exchange having previously been effected by an administrator level user who is able to validate the identity of the portable communication device to the computer device). Subsequent communications between the devices can then bypass the need for any key exchange. In such cases, symmetric cryptographic algorithms can be used since the secure exchange of keys has previously been effected. Thus for example initial communications between the computer device and the portable communication device can be the exchange of data tokens indicating the identity of the devices to one another, and subsequent data exchanges can be encrypted, the encryption key or keys having previously been exchanged.

The program means running on the computer device can for example be any application which is used to input credentials from a user in order for them to authenticate themselves. Thus for example the program means can for example be any desired logon/login application such as operating system logons (Win (RTM) Logon, Unix (RTM) Logon etc.), application logons such as website logons, email system logins, Oracle and SAP), and single sign-on (SSO) systems such as the Trinity product from Envoy Data Corporation and the v-GO product from Passlogix, Inc. (New York, USA).

The portable communication device has short-range wireless communication means which are capable of effecting data exchange with the short-range wireless communication means of the computer device.

Although portable communication devices such as mobile phones are already designed to create, store and use electronic credentials, this is only for use across a mobile phone network in order to e.g. authenticate the identity of a mobile phone to the network. As stated above, the present invention bypasses the need for the mobile phone network, and instead uses the short-range wireless communication abilities of the portable communication device to effect its authentication.

The portable communication device credentials store may be able to store multiple electronic credentials, for example of different types and strengths, and these may be usable with different applications (program means) on at least one computer device. So, for example, a computer device login may use a PKI (public key infrastructure) based electronic credential, whereas a website login may use an electronic credential based upon user ID and password. Similarly, a login for another program running on the computer device and which comprises an authentication module may use a previously-exchanged symmetric encryption/decryption key, or biometrics.

This can be particularly useful since it allows the portable communication device to act as an authentication store, storing multiple credentials for different systems with which it is to communicate. This means that where the portable communication device authentication module requires input from a user in order to enable transfer of a credential to a computer device then the portable communication device can simply prompt the user for a general authentication input (for example a PIN code, or a "Yes" in response to a request for confirmation that a credential should be transferred) irrespective of the credential which is to be transferred. Thus a user can use a single authentication input to validate transfer

of a range of credentials. Alternatively, the portable communication device may provide biometric reader functionality. For example, the portable communication device may comprise a fingerprint reader such as a Sony Puppy fingerprint reader. Examples of models include the FIU-900 which is a Sony memory-stick format device. The output from such a device may be used as user input to the authentication module of the portable communication device.

The portable communication device may, of course, allow for different authentication inputs for different sets of credentials stored in the credentials store, and the total number of stored credentials may be greater than the total number of authentication inputs.

The credentials store itself may be at least one of: an area of memory on the portable communication device, and an area of memory on the portable communication device SIM card.

The communication between the computer device authentication module and the portable communication device authentication module may effect the transfer of at least one credential from the portable communication device to the computer device.

The computer device can additionally comprise data input means, for example a keypad or a keyboard, mouse or a touch-screen device. The computer device may additionally comprise a user data input module. Thus the computer device may query the user for the input *via* the data input means of at least one additional authentication factor, and can process the response to the query in order to determine the authentication state.

The computer device of the present invention can allow for the input of data to confirm that data should be requested from the portable communication device.

When the short-range wireless communication means does not use line-of-sight communication (such as infra-red) then it can be desirable to ensure that any response received to the request from the computer device for authentication data is in fact from the correct portable communication device. For example, when using Bluetooth as the short-range wireless communication means, a large number of portable communication devices may receive the transmitted request. In order to ensure that any response is from the correct portable communication device, a challenge-response technique may be used in which either the user inputs data to the computer device to identify the portable communication device, or the computer device knows the identity of the correct portable communication device. With that information, a challenge block of data can be transmitted and responses verified against data held by the computer device in order to identify the correct portable communication device.

The last stages of the authentication process are the determination by the portable communication device of a response to the request for electronic credentials, the executing of the response by the portable communication device, and the processing of the response by the computer device to determine an authentication state. Depending upon how the portable communication device is configured, a range of responses may be available. For example, if the portable communication device detects that a credential is being requested which it does not have, it may provide no response to the request, or it may return a response indicating that the requested credential is not available. Where the requested credential is available then it may return an appropriate response including credentials data as appropriate.

The computer device authentication module may comprise a short-range communications manager, an authentication request processor and an authentication response processor. The short-range communications manager may manage communications over the short-range wireless communications device; the authentication request processor may effect the

request of at least one electronic credential from the portable communication device; and the authentication response processor may process any response from the portable communication device to extract any electronic credential in it.

The portable communication device authentication module may comprise a short-range communications controller, an authentication responder, a secure response processor, a credentials manager and a crypto manager. The short-range communications controller may effect the transfer of data from the portable communication device to the computer device; the authentication responder may determine from the data transmitted from the computer device the identity of a requested credential (for example, it may identify which application running on the computer device is requesting a credential); the credentials manager may effect the retrieval of credentials from the credentials store, and may request a user of the portable communication device to confirm that the requested credential should be transferred; the crypto manager may act to encrypt the credential returned from the credential store and pass it to the authentication responder such that when transmitted using the short-range wireless communication means, the encrypted credential can be decrypted by the computer device using a decryption key in its possession but cannot be readily decrypted without the decryption key; the authentication responder may act to transmit a response message to the computer device via the short-range wireless communication means.

Thus the portable communication device authentication module may process the request for electronic credentials, retrieve any relevant electronic credentials, formulate a response to the request for electronic credentials, and transmit the response to the computer device *via* the short-range wireless communication means.

Thus the authentication state may be determined by the computer device authentication module effecting communications with the portable communication device *via* the short-

range wireless communication means, transmitting the request for electronic credentials, and processing the response to the request for electronic credentials to determine the authentication state.

In particular, the computer device authentication module comprising a short-range communications manager, an authentication request processor and an authentication response processor, can instruct:

(i) the short-range communications manager to effect communications with the portable communication device *via* the short-range wireless communication means;

(ii) the authentication request processor to instruct transmission of the request for electronic credentials; and

(iii) the authentication response processor to process the response to the request for electronic credentials to determine the authentication state.

The present invention also provides the ability to allow the portable communication device to establish a VPN (virtual private network) session with a remote computer across a mobile phone network connection. Thus, for example, upon the authentication of a user to the computer device, the computer device can initiate a connection with a remote network across a mobile phone network using the portable communication device. For example, the authentication step can be the establishment of a VPN session. This VPN session can be established using the portable communication device, the session being established across a mobile phone network (as above) or it can be established *via* an alternative network connection not provided by the portable communication device, e.g. a network access point such as a WiFi connection or a wired network connection. This use of the portable communication device to authenticate the user of the computer device means that not only must the user be in possession of the computer, but also the portable communication device in order to effect the VPN connection. In addition, the computer

device and/or the portable communication device may require a further authentication factor such as a secret to be provided by the user.

Network access points are points to which a computer device can connect in order to gain access to a network, particularly to the internet. Examples of network access points are: a telephone socket for a modem connection to the internet over a telephone line; a broadband connection point for a cable modem or access *via* a cable TV set-top box; and a local area network (LAN) socket, either wired or wireless (WLAN).

Another aspect of the present invention is that in supplying an electronic credential to the computer device, the portable communication device can act to digitally sign data for the purposes of non-repudiation. Thus for example upon the authentication of a user to the computer device upon the basis of an electronic credential supplied by the portable communication device, data for digitally signing could then be passed to the portable communication device, which could then effect its signing and return the signed data to the computer device. So for example the contents of an email could be passed to the portable communication device for digital signature, and it could then be returned to the computer device for sending to third parties.

The invention will be further apparent from the following description, with reference to the several figures of the accompanying drawings, which show, by way of example only, one form of apparatus and method for authenticating a user to a computer device. Of the Figures:

Figure 1 shows the general interactions between the user, computer device and portable communication device to effect authentication;

Figure 2 shows the component parts of the computer device used in authenticating a user to it;

Figure 3 shows the component parts of a portable communication device used in effecting authentication of a user to a computer device;

Figure 4 shows an architecture of a VPN (virtual private network) connection effected from the computer device *via* the portable communication device which also effects authentication of the user to the computer;

Figure 5 shows an alternative architecture of a VPN connection with authentication of a user being effected *via* the portable communication device, but with the computer device using alternative network communication means (e.g. a LAN connection) to establish a VPN connection; and

Figure 6 shows the digital signing of a document on a computer device using a credential supplied by a portable communication device.

Authenticating to a Computer Application

As shown in Figure 1, a person 1 wishes to access a computer application 3 on a computer device 2, e.g. the computer device login. The person 1 initiates the start-up of the computer application 3 and positions their mobile phone 6 within wireless range of computer device 2. Computer application 3 requests the person 1 to input their electronic credentials of the specific type required for application 3, before access to it is allowed. At this point computer device authentication module 4 enables a short-range wireless connection 5 and transmits a request for electronic credentials across the short-range wireless connection 5 to a phone authentication module 7 on the mobile phone 6.

The phone authentication module 7 presents a notification of the request to the person 1 and asks them to confirm the request to transmit electronic credentials. On confirming the request, phone authentication module 7 then retrieves the previously stored electronic credentials 8 from the mobile phone 6 and transmits them back to the computer device 2 using the short-range wireless connection 5.

On receipt of the electronic credentials 8, the computer device authentication module 4 structures and presents them back to the computer application 3 in the required format, authentication is effected and access to the application is granted/denied as appropriate.

The above processes are described in further detail below.

Apparatus:

Computer Device

Computer device 2 shown in Figure 2 is a laptop computer running Windows (RTM). It is capable of establishing a short-range wireless connection 5 using Bluetooth (RTM) across a wireless interface 23.

As is shown in Figure 2, computer device authentication module 4 is a computer program forming an integral part of computer application 3. In other embodiments of the present invention, computer device authentication module 4 is a discrete application on computer device 2 which interfaces with computer application 3.

Computer device authentication module 4 comprises the following components:

- a short-range communications manager 20;
- an authentication request processor 21; and
- an authentication response processor 22.

The person 1 using computer device 2 interfaces with computer application 3 and computer device authentication module 4 by means of display 24 which displays messages, and by keyboard 25 which is used for keying in responses to the messages. Communication between computer device 2 and mobile phone 6 is effected (on the side of computer device 3) *via* wireless interface 23 and short-range wireless connection 5.

Configuration of the Mobile Phone

Figure 3 shows mobile phone 6 which is capable of connecting to a mobile (or cell) phone network for the purpose of making person to person or person to information (Internet) calls. Mobile phone 6 has an Operating System 37, namely the Symbian (RTM) OS, which is capable of performing cryptographic functions and storing electronic credentials in memory on mobile phone 6. Mobile phone 6 is also capable of effecting a short-range wireless connection 5 using Bluetooth (RTM) across a wireless interface 36.

As can be seen from Figure 3, mobile phone 6 comprises a phone authentication module 7 (which is a computer program that runs on mobile phone 6), a credentials store 35, a wireless interface 36, an OS 37, a keypad 38 and display 39. Phone authentication module 7 comprises:

- a short-range communications controller 30;
- an authentication responder 31;
- a secure response processor 32;
- a credentials manager 33; and
- a crypto manager 34.

Phone authentication module 7 interfaces with the person 1 using the mobile phone 6 by means of display 39, and by keypad 38. The credentials store 35 is an area of memory on the mobile phone. Communication between the mobile phone and the computer device is effected *via* wireless interface 36 and short-range wireless connection 5.

In use, and as shown by Figures 2 and 3, computer device authentication module 4 on computer device 2 is executed whenever computer application 3 shows a message on display 24 requesting person 1 to present their electronic credentials. When the request for electronic credentials is made, computer device authentication module 4 instructs short-range communications manager 20 to enable wireless communications *via* wireless interface 23.

Computer device authentication module 4 then instructs authentication request processor 21 to request the electronic credentials for computer application 3. In the event that the authentication request involves digitally signing data, then the authentication request includes the data to be signed. Authentication request processor 21 transmits a request *via* wireless interface 23 and short-range wireless connection 5 to phone authentication module 7 on mobile phone device 6.

Phone authentication module 7 receives the request from computer device authentication module 4 where it is intercepted by authentication responder 31 which determines from the request which application is requesting the electronic credentials and instructs credentials manager 33 to retrieve the electronic credentials for that application.

Credentials manager 33 then sends a message to mobile phone display 39 asking person 1 to confirm the request to retrieve electronic credentials from credential store 35. The person confirms the request by typing in the appropriate response using keypad 38. The nature of the confirmation may vary - where the credentials are PKI based this can be e.g. a pass-phrase used to gain access to the private key, or if a UserID and password then a simple key depression may suffice.

On receipt of confirmation, credentials manager 33 retrieves the electronic credentials from credentials store 35 and instructs crypto manager 34 to perform the appropriate

action. If the authentication request involves signing then crypto manager 34 will digitally sign the data in the authentication request using the private key and certificate retrieved from credentials store 35. If the authentication request involves an encrypted UserID and password then crypto manager 34 decrypts them.

Control is then passed to secure response processor 32 that protects the message to be sent back to computer device 2, such that the credentials are not revealed if intercepted by another person's wireless device. Secure response processor 32 passes the response message to authentication responder 31, which in turn sends it back *via* wireless interface 36 and wireless connection 5 to computer device authentication module 4.

Authentication response processor 22 intercepts the authentication response message. It then reformats the response message so that the credentials can be passed to computer application 3 in the required format - this can include removing the protection added by the mobile phone 6 secure response processor 32.

Finally, authentication response processor 22 responds to the authentication request from computer application 3, and person 1 gains access to the computer application, or is denied access as appropriate.

Establishing a VPN Session *via* the Mobile Phone

As shown in Figure 4, having completed the authentication to computer device 2, a person 1 may wish to establish a VPN session 40 with a remote network 41. Person 1 initiates VPN session 40 from computer device 2, which sends a command across short-range wireless connection 5 to initiate the modem function of mobile phone 6, and establishes an Internet connection 42 with remote network 41. This in effect creates a seamless electronic channel between computer device 2 and remote network 41.

On establishing this channel, remote network 41 requests person 1 to present their electronic credentials 8 at computer device 2. Using short-range wireless connection 5, the person accesses electronic credentials 8 on mobile phone 6 and presents these to remote network 41. On confirming the authenticity of the credentials and therefore the authentication of computer device 2, remote network 41 establishes VPN session 40 between computer device 2 and the remote network 41.

Establishing a VPN Session *via* a Network Access Point

As shown in Figure 5, an alternative to establishing a VPN session 40 *via* internet connection 42 provided through mobile phone 6 is to use an alternative network access point. Upon completing authenticating to computer device 2, person 1 connects to network access point 43 (a cable connection) to establish an Internet connection 42 with remote network 41. Remote network 41 requests person 1 to present their electronic credentials 8 at computer device 2. Using short-range wireless connection 5, person 1 accesses the electronic credentials 8 on the mobile phone 4 and presents these to computer network 41. On confirming the authenticity of credentials 8 and hence of computer device 2, remote network 41 establishes VPN session 40 between itself and computer device 2.

Digitally Signing For Non-Repudiation

As shown in Figure 6, person 1 wishes to sign electronic document 11 on computer device 2. The computer application 3 used to do this on computer device 2 is signing computer application 10, and it digitally signs electronic document 11 using electronic credentials 8 stored on mobile phone 6.

It will be appreciated that it is not intended to limit the invention to the above example only, many variations, such as might readily occur to one skilled in the art, being possible, without departing from the scope thereof as defined by the appended claims.

CLAIMS

1. Apparatus for effecting authentication to a computer device, comprising:

(a) a computer device comprising:

(i) short-range wireless communication means; and

(ii) program means comprising a computer device authentication module for communicating with a remote device using said short-range wireless communication means and authenticating said remote device;

(b) a portable communication device comprising:

(i) mobile phone network communication means;

(ii) short-range wireless communication means;

(iii) program means comprising a portable communication device authentication module for communicating with said computer device using said short-range wireless communication means; and

(iv) data storage means providing a credentials store for storing authentication data.

2. Apparatus according to claim 1, said computer device additionally comprising data input means.

3. Apparatus according to claim 2, said data input means being selected from the group consisting of keyboard, mouse and touch-screen.

4. Apparatus according to any of the preceding claims, said computer device program means additionally comprising a user data input module.

5. Apparatus according to claim 1, said computer device authentication module comprising a short-range communications manager, an authentication request processor and an authentication response processor.

6. Apparatus according to any of the preceding claims, said portable communication device authentication module comprising a short-range communications controller, an authentication responder, a secure response processor, a credentials manager, and a crypto manager.

7. A method for effecting authentication to a computer device using a portable communication device, said computer device comprising:

(i) short-range wireless communication means;

(ii) program means comprising a computer device authentication module for communicating with a remote device using said short-range wireless communication means and authenticating said remote device; and

(iii) data storage means for storing reference data against which authentication is to be effected;

and said portable communication device comprising:

(i) mobile phone network communication means;

(ii) short-range wireless communication means;

(iii) program means comprising an authentication module for communicating with said computer device using said short-range wireless communication means; and

(iv) data storage means providing a credentials store for storing authentication data;

said method comprising the steps of:

(a) transmitting a request for electronic credentials *via* said short-range communication means from said computer device to said portable communication device;

(b) with said portable communication device authentication module, processing said request for electronic credentials, determining a response to said request for electronic credentials based upon said authentication data, and executing said response; and

(c) with said computer device, processing said response to said request for electronic credentials to determine an authentication state.

8. A method according to claim 7, said step of executing said response comprising transmitting a response message *via* said short-range wireless communication means from said portable communication device to said computer device.

9. A method according to either of claims 7 or 8, said computer device additionally comprising data input means, said method additionally comprising with said program means querying said user for input *via* said data input means of at least one additional authentication factor, and processing the response to said query to determine said authentication state.

10. A method according to claim 9, said data input means being selected from the group consisting of keyboard, mouse and touch-screen.

11. A method according to any of claims 7-10, said program means additionally comprising a user data input module.

12. A method according to any of claims 7-11, said computer device authentication module effecting communications with said portable communication device

via said short-range wireless communication means, transmitting said request for electronic credentials, and processing the response to said request for electronic credentials to determine said authentication state.

13. A method according to claim 12, said computer device authentication module comprising a short-range communications manager, an authentication request processor and an authentication response processor, said computer device authentication module instructing:

(i) said short-range communications manager to effect communications with said portable communication device *via* said short-range wireless communication means;

(ii) said authentication request processor to instruct transmission of said request for electronic credentials; and

(iii) said authentication response processor to process the response to said request for electronic credentials to determine said authentication state.

14. A method according to any of claims 7-13, said portable communication device authentication module processing said request for electronic credentials, retrieving any relevant electronic credentials, formulating a response to said request for electronic credentials, and transmitting said response to said computer device via said short-range wireless communication means.

15. A method according to claim 14, said portable communication device authentication module comprising a short-range communication controller, an authentication responder, a secure response processor, a credentials manager and a crypto manager.

Application No: GB0326594.9 **Examiner:** Dr Russell Maurice

Claims searched: all **Date of search:** 7 February 2005

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	all	WO 00/31608 A2 (ERICSSON) see eg the Abstract and page 2 line 14 - page 3 line 6
X	all	WO 02/095689 A1 (ERICSSON) see eg the Abstract and page 4 lines 5-9, page 5 line 5-8 & 21-24
X	1 & 7 at least	JP 10228327 A (NITE) see WPI Abstract Accession Number 1998-516515 [44]
A	-	US 2002/0078362 A1 (NEC) see eg the Abstract
A	-	WO 02/32151 A2 (LCI/SMARTPEN) see eg the Abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

G4H

Worldwide search of patent documents classified in the following areas of the IPC[07]

G06F

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, PAJ